HHS | Hart Health Strategies

HIPAA Final Omnibus Rule: What Physicians Need to Know

Background

On January 25, 2013, the Department of Health and Human Services (HHS) published its Omnibus Health Insurance Portability and Accountability Act (HIPAA) final rule implementing changes aimed at increasing patient privacy and securing health information as required under the Health Information Technology for Economic and Clinical Health Act (the HITECH Act).

The final omnibus rule is the resultant outcome of previous interim final and proposed rulings that have been released over the course of the last several years, including the following:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Breach Notification Rule
- HIPAA Enforcement Rule

The final omnibus rule became effective on March 26, 2013, with a compliance date of September 23, 2013.

Business Associates

Expanded Definition of Business Associates

The final omnibus rule modifies the definition of "Business Associates" (BA) to include a number of new organization types including patient safety organizations (PSOs), health information exchanges (HIEs) and regional health information organizations (RHIOs), as well as personal health record (PHR) vendors, document storage entities, and e-prescribing gateways. Other organizations that provide data transmission services requiring access to protected health information (PHI) on a routine basis are also considered business associates. In addition, subcontractors that perform services on behalf of a business associate are now included in the definition of business associates, and therefore, must comply with most HIPAA requirements.

New Liabilities for Business Associates

Business associates are now required to comply with certain aspects of the HIPAA Privacy, Security and Breach Notification Rules. With regard to the Security Rule, business associates must implement administrative, physical, and technical safeguards to protect PHI, as well as implement policies and procedures, and maintain documentation demonstrating compliance. With regard to the Privacy Rule, business associates are now directly liable for uses and disclosures of PHI. HHS will also require business associates' compliance with the "minimum necessary standard" (Note: HHS intends to issue more guidance on the minimum necessary standard for Bas in the future). Regarding the Breach Notification Rule, business associates are required to provide notice of breaches to physician practices not later than 60 days following discovery of the breach.

Business Associate Agreements

Physician practices must update their business associate agreements in light of the final rule. New BA agreements must comply with the final rule by September 23, 2013; whereas existing

agreements must be modified to meet the new requirements by September 22, 2014. A sample Business Associate agreement that reflects modifications described in the final rule has been posted on the HHS Office of Civil Rights (OCR) website. Physician practices should ensure that new and updated agreements accurately reflect business arrangements with their business associates.

Privacy & Security

Notice of Privacy Practices

Physician practices must update their Notice of Privacy Practices to comply with new requirements described in the final rule not later than September 23, 2013. Revised Notice of Privacy Practice's must include the following statements:

- That an individual has the right to restrict disclosures of PHI to health plans if the individual has paid for services out of pocket in full;
- That use and disclosure of PHI will only be made with authorization from the individual if the data would be would be used or disclosed for marketing purposes;
- That use and disclosure of PHI will only be made with authorization from the individual if the data would constitute a sale of PHI;
- That an individual has a right to opt out of fundraising communications; and,
- That other uses and disclosures not described in the Notice will be made only with authorization from the individual.

In addition, the Notice must include a statement of the right of an affected individual to be notified following a breach of unsecured PHI.

If they so choose, physician practices may remove previously required statements that the covered entity may contact the individual with appointment reminders or information about treatment alternatives or other health-related benefits or services.

The revised Notice must be posted both to the provider's website (if they have a website) and in a prominent location (such as in the patient waiting room). The revised Notice must be made available to existing patients upon request, and new patients must be provided with a copy of the revised notice beginning September 23, 2013.

Expanded Patient Access to PHI

According to the final rule, physician practices that use or maintain an electronic health record (EHR) must allow individuals to obtain a copy of their health information in an electronic format or have an electronic copy transmitted to their designee. Fees associated with the transmission must not be greater than the physician practice's labor costs in responding to the request. Health information that is stored electronically (such as in a PDF, HTML or other file) but not used and maintained as part of an EHR must also be accessible by individuals.

Physician practices may continue to require that individuals make requests for PHI in writing. Requests for PHI must be answered within 30 days, with a one-time extension of up to 30 days. The 30-day window is triggered at the time the request for PHI is made.

Right to Request Certain Restrictions

With few exceptions, individuals may now restrict certain disclosures of PHI to their health plan if the individual (or someone on their behalf, such as a family member) pays out of pocket in full for healthcare items or services. Physician practices should develop a mechanism by which they can "flag" PHI that has been restricted by an individual so that the information is not inadvertently sent to a health plan for payment, health care operations, or in the event of an audit.

In instances where state or other laws require a provider to submit a claim and there is no exception for those paying out of pocket, the physician practice may disclose the PHI to the health plan. Disclosures may also be made if they are part of a CMS Conditions of Participation survey. In addition, if an individual does not make payment for the healthcare items or services (for example, if the individual's payment is dishonored by their financial institution) the practice should make a reasonable attempt to collect the amount due before submitting a claim to the individual's health plan.

Breach Notification

Risk Assessments

The previous "Risk of Harm" analysis has been eliminated and replaced with a "Risk Assessment" approach. Under this approach, breach notification is not required if the physician (or its business associate) can demonstrate through a risk assessment that there is a low probability that the PHI has been compromised. The final rule explains that the risk assessment should consider a combination of the following factors:

(1) The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
(2) The unauthorized person who used PHI or to whom PHI was disclosed;
(3) Whether PHI was actually acquired or viewed; and,
(4) The extent to which the risk to PHI has been mitigated.

If the physician practice determines that the unauthorized disclosure was not a breach, it should maintain documentation to overcome the presumption of a breach. If a physician practice decides to notify individuals of the unauthorized disclosure, it would not be required to conduct the risk assessment.

Physician practices are required to notify the Secretary of all breaches of unsecured PHI affecting few than 500 individuals not later than 60 days after the end of the calendar year in which the breaches were discovered. Breaches affecting more than 500 individuals must be reported to the Secretary immediately.

If a business associate is acting as an agent on behalf of the physician practice, then the business associate's discovery will be imputed to the physician practice. The physician practice must notify HHS of breaches within a certain allotted time measured by when its business associate discovered the breach, not when the physician practice became aware. New and updated BA contracts should address how and when the business associate will notify the physician practice of a suspected breach.